United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, D.C. 20240

OCIO DIRECTIVE 2004 - 018

To: Heads of Bureaus and Offices
Chief Information Officers

From: W. Hord Tipton
Chief Information Officer

APR 0 8 2004

Subject: Prohibition on Use of Wireless Network Technology

Wireless networks (WLANs) have gained popularity in modern networks with many benefits including convenience, portability, increased productivity, inexpensive, and easy implementation. However, these benefits are not without considerable risk to the Department of the Interior (DOI). Desirable benefits of usability and productivity in WLANs are also what present significant challenges for DOI implementing WLANs in a secure fashion.

Denial of service attacks, session hijacking, and password and data sniffing are just a small sample of the potential threats we face. While many of the attacks against wireless networks are similar to those against wired networks, 802.11xx networks are generally subject to more threats. One of the more serious problems is Wired Equivalent Privacy (WEP), the data encryption standard for wireless networks. WEP has been found to have weaknesses and is easily compromised. Sophisticated tools already exist for non-sophisticated users to take advantage of this vulnerability and gain access to potentially sensitive data transmissions.

Due to the significant security risks associated with wireless technology, DOI does not authorize the use of any 802.11xx devices. This includes accessing DOI systems from home wireless networks. If wireless networks currently exist, bureaus and offices must immediately disconnect them from DOI wired networks.

A limited number of pilot projects may be instituted with approval by Interior's Chief Information Officer (CIO). Bureaus implementing an approved pilot must have security mechanisms in place and implement the security controls outlined in the DOI 802.11xx Wireless Security Technical Implementation Guide (STIG). Bureau CIOs must submit a written report to the Office of the CIO identifying existing wireless deployments within 30 days of the issuance of this directive. Also included in the report should be affirmation that wireless systems have been shut down.

If you have any questions regarding this directive, please contact me at (202) 208-6194. Staff may contact Roger Mahach, Departmental Chief Information Security Officer, at the same number.